

#16 - UNLAWFUL INTERNET GAMBLING WORKPROGRAM

ASSIGNMENT OVERVIEW

The Unlawful Internet Gambling Enforcement Act (UIGEA) prohibits gambling businesses from knowingly accepting payments in connection with the participation of another person in a bet or wager involving the use of the Internet, if it is unlawful under applicable law. Such payments are called “restricted transactions”. The rule requires certain participants in the designated payment systems (ACH, card systems, check collection, money transmitting businesses, and wire transfer) to establish policies and procedures that are reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions.

The final rule focuses on preventing unlawful Internet gambling businesses from benefitting from the payment system by denying them the opportunity to open bank accounts from which to receive payments.

The final rule requires a strengthened screening process at the time of account opening to deny commercial entities that may be acting as Internet casinos access to the payments system. It also requires that policies and procedures be implemented to prevent all debit and credit card payments to Internet casinos. It does not require that checks, ACH payments, or wire transactions related to Internet gambling be monitored or blocked.

The regulation requires compliance in four general areas:

1. Screening commercial customers at account opening;
2. Policies and procedures to identify and block restricted transactions;
3. Policies and procedures to follow when the bank has knowledge that a commercial customer engages in an Internet gambling business; and
4. Notice requirements for existing commercial account customers.

For more information see 12 CFR Part 233 and FRB SR 10-11 which are found in the [Appendix](#).

CORE ANALYSIS

UIGEA compliance examination should be risk-focused. In tailoring the scope of the examination work, examiners may consider appropriate risk factors, such as the number of commercial accounts the institution maintains for commercial customers engaged in the business of internet gambling. If the institution is not using the safe harbor policies and procedures as set forth in the rule (12 CFR Part 233) and as assumed in the examination procedures below, examiners must determine whether the institution's policies and procedures are reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions.

1. Qualification as Non-Exempt Participant

1a. Determine whether the institution qualifies as a non-exempt participant in a designated payment system as defined by the provisions of the UIGEA. *See chart in [Appendix](#).*

A "participant" is defined as "an operator of a designated payment system, a financial transaction provider that is a member of, or has contracted for financial transaction services with, or is otherwise participating in, a designated payment system, or a third-party processor.

Typically, if an institution operates or participates in a credit/debit card program, or ACH/wire transfer system, they are non-exempt and subject to the rules.

Comment:

2. Risk Assessment and Audit Reports

2a. Obtain and review any risk or other assessments and audit reports that assess the institution's UIGEA compliance. Determine whether deficiencies noted in the last examination and most recent internal/external audit have been addressed and/or corrected by management. Detail how deficiencies were corrected. *Include copy of exam and/or audit exceptions and management response, if applicable. Comment on any deficiencies noted.*

Comment:

2b. Determine which position in the institution is responsible for UIGEA compliance. *Identify employee name and title.*

Comment:

3. Policies and Procedures for UIGEA

3a. Review/determine the adequacy of the institution's policies and procedures for determining whether a commercial customer presents more than a minimal risk of engaging in an Internet gambling business (*due diligence*). *Comment on any weaknesses or deficiencies. Refer to [Appendix](#) for guidance.*

Comment:

3b. Review/determine the adequacy of the institution's policies and procedures for obtaining documentation from commercial customers who present more than minimal risk of engaging in an Internet gambling business, or when the institution has actual knowledge that the customer is engaged in such a business. Documentation includes:

1. A certification from the customer that it does not engage in an Internet gambling business; or
2. If the customer does engage in Internet gambling business:
 - a. Either a copy of the commercial license from a State or Tribal authority authorizing the customer to engage in the business or a reasoned legal opinion that demonstrates that the business does not involve restricted transactions; and
 - b. A written commitment by the customer to advise the participant of any changes in its legal authority to engage in the Internet gambling business; and
 - c. A third-party certification that the customer's systems for engaging in the Internet gambling business are reasonably designed to ensure that the business will remain within legal limits.

Note: If the bank's policy is modeled on the guidance, these statements will be included.

Comment:

3c. If applicable, determine whether the institution appropriately uses a code system for card transactions to detect potential restricted transactions. *This is typically performed by the card system operator.*

The bank is in compliance with the rule if one of the following is true:

1. *New account due diligence processes are in place, and notice has been provided to all commercial account holders; or*
2. *The bank is relying on the card system provider to comply with the rule.*

If the bank does not have a new account due diligence processes in place and is relying on the system operator's compliance with the rule, the bank should obtain a written statement from the system operator stating that the operator is in compliance with the UIGEA.

Comment:

3d. Determine whether the institution has in place:

1. An adequate mechanism to receive notice (e.g. from law enforcement or supervisory authorities) that restricted transactions have been sent through an account at the institution and
2. Policies and procedures to be followed when the bank receives such actual knowledge of restricted transactions.

Comment:

3e. Review /determine the adequacy of any procedures or measures established by the institution to determine the circumstances under which the institution should deny service, close an account, report suspicious activity, conduct an account review, or continue transaction processing in instances of actual knowledge of restricted transactions. *Comment on any weaknesses or deficiencies.*

Comment:

3f. Determine whether the institution has taken appropriate steps to provide written notice (as part of an account agreement, on the institution's website or otherwise) to all commercial accountholders that accounts may not be used for restricted transactions. The notice to all existing commercial accountholders was required by June 1, 2010.

Comment:

3g. Determine whether the institution has incorporated UIGEA compliance measures into its processes for managing correspondent account relationships.

The rule generally covers payments flowing through foreign correspondent relationships. For example, a correspondent bank that participates in wire transfer transactions is non-exempt when it is acting as the beneficiary's bank. If a U.S. depository institution establishes a correspondent account for a foreign financial institution that will involve designated payment system(s) for which the U.S. bank will be a non-exempt participant, the U.S. bank must have policies and procedures in place as required by the rule.

Comment:

4. Final Analysis

4a. Complete the [Summary of Findings](#) page.

SUMMARY OF FINDINGS

#16- UNLAWFUL INTERNET GAMBLING

Describe all strengths evident from the evaluation.

Describe all weaknesses evident from evaluation, including violations of law/regulation/rules; noncompliance with Departmental policies/guidelines; internal policy deficiencies/ noncompliance; internal control weaknesses; MIS problems; and deficiencies in management supervision.

Report Worthy:

Not Report Worthy:

Determine why weaknesses exist and comment on management's response and plan of action. Identify bank personnel making the response.

SUMMARY RISK RATING ASSIGNED:

Definitions:

1-Strong; 2-Satisfactory; 3-Less than satisfactory; 4-Deficient; 5-Critically deficient; NR-Not Rated

 [\(Return to Core Analysis\)](#)

Provide copy of this page to EIC/AEIC. Receipt and review of this form by the EIC/AEIC will be evidenced by his/her initials in the appropriate column for this procedure on the SCOPE AND WAIVER FORM (Planning and Control Worksheet #1).

APPENDIX

UIGEA, Designated Payment Systems and Requirements of Participants

Payment System	Non-Exempt Participants	Safe Harbor Policies and Procedures: General Requirements
Card Systems (credit, debit, stored value)	<ol style="list-style-type: none"> 1. Card issuers 2. Merchant acquirers 3. Operators 4. Third-party processors 	<ul style="list-style-type: none"> • Due diligence <u>or</u> • Use of codes to identify restricted transactions and ongoing monitoring for codes; <u>and</u> • Restricted transactions procedures.
Automated Clearing House (ACH)	<ol style="list-style-type: none"> 1. RDFI, credit transactions 2. ODFI, debit transactions 3. Gateway operator for cross-border debits 4. Third-party processors for any of 1,2 or 3 	<ul style="list-style-type: none"> • Due diligence • Restricted transaction procedures; <u>and</u> • For inbound cross-border ACH debit transactions, notice to correspondent bank in case of actual knowledge of restricted transactions.
Wire Transfer	Beneficiary's bank	<ul style="list-style-type: none"> • Due diligence <u>and</u> • Restricted transactions procedures.
Check Collection	<ol style="list-style-type: none"> 1. Depository bank 2. First U.S. bank for cross-border check receipts 	<ul style="list-style-type: none"> • Due diligence; • Restricted transactions procedures; <u>and</u> • For cross-border transactions, notice to correspondent bank in case of actual knowledge of restricted transactions.
Money Transmitting Businesses	Operators of money transmitting businesses that permit initiation of funds transmissions remotely, such as via Internet or telephone.	<ul style="list-style-type: none"> • Due diligence; • Ongoing monitoring by the operator to detect potential restricted transaction; <u>and</u> • Restricted transactions procedures.

“Due diligence” includes the following:

- Written notice to all commercial account holders that the account must not be used for restricted transactions;
- Risk assessment for each commercial account opened on or after the rule's compliance date to determine whether the accountholder poses more than a minimal risk of engaging in restricted transactions; and
- Obtaining as required documentation if the commercial customer presents more than a minimal risk of engaging in an Internet gambling business and cannot certify that it is not so engaged or if the institution has actual knowledge that a commercial accountholder is engaged in an Internet gambling business.

“Restricted transactions procedures” are to be followed when an institution has actual knowledge that a commercial customer has received funds in a restricted transaction. Procedures should address continued transaction processing, account review, SAR filing, and account closure.

 [\(Return to Core Analysis\)](#)

APPENDIX

3. Bank Policy and Procedures

1. The policy should demonstrate the steps the bank is taking to prevent a commercial entity engaged in Internet gambling from opening an account.

Steps when a new customer applies to open an account should include:

1. Determine whether the account is for an individual or a commercial entity. If it is for an individual no further action is required under the UIGEA final rule.
2. If it is a commercial entity, the bank, as part of its normal due diligence, should assess whether there is a “minimal risk” of it acting as an Internet gambling business. If so, then no further action is required under the UIGEA final rule.
3. If a bank is not able to determine if a commercial applicant has a “minimal risk” of acting as an Internet gambling business, they can rely on the applicant’s own certification that they do not operate as an Internet gambling business.
4. If a bank determines that an applicant does operate an Internet gambling business, it can still open the account if additional standards are met including:
 - Requiring the applicant to provide evidence of their legal authority to offer online gaming. This evidence could be in the form of a state issued license or an attorney’s legal opinion, and
 - The commercial entity is required to provide a third party certification that its Internet gambling business has controls in place to prevent improper use of the site by minors or from other individuals in other geographic locations where such gambling would be prohibited and the Internet gambling business must provide the bank regarding any changes in status of its legal authority to operate.

(The rule does not require a bank to re-investigate existing commercial customers but does mandate that disclosures be made to existing commercial customers regarding the UIGEA’s restrictions).

2. The policy should require notice to existing commercial account holders that restricted transactions are prohibited from being processed through the account or relationship. Indicate what form of notice is provided (*Account agreement or separate notice or website*) in the comments for Q3a.

[➤ \(Return to Core Analysis\)](#)

APPENDIX

UIGEA RESOURCES

12 CFR Part 233



12 CFR Part 233.pdf

SR 10-11 and Unlawful Internet Gambling Enforcement Act of 2006 – Overview (May 20, 2010)



SR 10-11.pdf



Unlawful Internet
Gambling.pdf

[➤ \(Return to Core Analysis\)](#)